IN THE CLAIMS:

This listing of claims will replace all prior versions, and listing, of claims in the application.

Listing of the Claims:

1. (Currently amended) A method of communicating an electronic document between a first and second security domain[[s]]], ~~wherein a~~ each security domain ~~comprises~~comprising a network having a common level of resilience to security threats, the method comprising the steps of:

receiving, in [[a]]the first security domain, a request to transmit to [[a]]the second security domain a first electronic document in a first data format capable of supporting one or more covert security threats, said security threats comprising presence in the first document of malicious code;

forwarding the first electronic document via at least one of a firewall and a data diode to a computerized format converter;

~~creating~~ applying the computerized format converter to the first electronic document whereby to create a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document, wherein creating said second document comprises adding at least one of entropy and randomness to a least one characteristic of the representation of the first document; and

forwarding the second document in place of the first document to the second security domain.

2. (Previously presented) A method according to claim 1 in which forwarding the second document is conditional upon sanction.

3. (Currently amended) A method according to claim 1 in which the second document is digitally ~~singed~~signed by a sanctioning user.

4. (Currently amended) A method according to claim 1 in which the second document is forwarded to the second security domain via a second at least one of a firewall and a data diode.

5. (Previously presented) A method according to claim 1 in which the step of creating the second document comprises performing a transformation to the first document which modifies the underlying data format of the document whilst preserving the visible informational content.

6. (Cancelled)

7. (Currently amended) A method according to claim [[6]]1 in which the at least one characteristic comprises at least one of colour and spacing.

8. (Previously presented) A method according to claim 1 in which the step of creating the second document comprises applying a lossy compression method.

9. (Previously presented) A method according to claim 1 comprising the step of:

conveying the second document to a user sanction function for review and sanction prior to sending the second document to the second security domain.

10. (Previously presented) A method according to claim 1 in which review and sanction comprises sanction by a human user.

11. (Cancelled)

12. (Currently amended) A method according to claim 11 in which the malicious code comprises at least one of a computer virus, a worm, ~~and~~ a Trojan horse, a back door attack, a BIOS attack, a microcode malware attack, social engineering attack, and buffer overflow attack.

13. (Previously presented) A method according to claim 1 in which the one or more security threats comprises data steganographically concealed within the first document.

14. (Previously presented) A method according to claim 1 in which the first security domain and second security domain are rated at different security levels.

15. (Previously presented) A method according to claim 1 in which the first security domain is a lower-level security domain than the second security domain.

16. (Previously presented) A method according to claim 14 in which the first security domain is a higher-level security domain that the second security domain.

17-21. (Cancelled)

22. (Currently amended) Apparatus for communicating an electronic document between security domains, wherein a security domain comprises a network having a common level of resilience to security threats, the apparatus comprising:

first computerized apparatus arranged to receive, in a first security domain, a request to transmit to a second security domain a first electronic document in a first data format capable of supporting one or more covert security threats;

computerized format converter apparatus arranged to create a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document, wherein creating said second document comprises adding at least one of entropy and randomness to at least one characteristic of the representation of the first document;

second apparatus comprising at least one of a firewall and a data diode, arranged to receive the first and second electronic document from the first computerized apparatus and forward it to the format converter; and

apparatus arranged to forward the second document in place of the first document to the second security domain.

23. (Currently amended) Apparatus according to claim 22 implemented as a[[A]] computer chipset ~~for communicating an electronic document between security domains, wherein a security domain comprises a network having a common level of resilience to security threats, the computer chipset comprising:~~

~~a first component arranged to receive, in a first security domain, a request to transmit to a second security domain a first electronic document in a first data format capable of supporting one or more covert security threats;~~

~~a second component arranged to create a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document, wherein creating said second document comprises adding at least one of entropy and randomness to at least one characteristic of the representation of the first document; and~~

~~a third component arranged to forward the second document in place of the first document to the second security domain~~.

24. (Currently amended) A non-transitory computer readable medium having program code recorded thereon to direct a computer to communicate an electronic document between a first and a second security domain[[s]], ~~wherein a~~each security domain ~~comprises~~comprising a network having a common level of resilience to security threats, the program code comprising:

a first code portion arranged to receive, in a first security domain, a request to transmit via at least one of a firewall and a data diode to a second security domain a first electronic document in a first data format capable of supporting one or more covert security threats comprising presence in the first document of malicious code;

a second code portion arranged to create a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document, wherein creating said second document comprises adding at least one of entropy and randomness to at least one characteristic of the representation of the first document; and

a third code portion arranged to forward the second document in place of the first document to the second security domain.

25. (New) A method according to claim 4 in which the at least one of a firewall and a data diode is a data diode and in which the second at least one of a firewall and a data diode is a data diode.